PRUDENTIAL STANDARD
FOR THE MANAGEMENT OF OPERATIONAL RISK
FOR INSTITUTIONS LICENSED UNDER THE BANKING ACT 2015

EASTERN CARIBBEAN CENTRAL BANK
ST KITTS

TABLE OF CONTENTS

BANKING PRUDENTIAL STANDARDS NO. 01 OF 2020

This standard is issued by the Eastern Caribbean Central Bank (Central Bank), in exercise of the powers conferred on it by Section 184 of the Banking Act, No.…of 2015[1] (hereinafter referred to as the Act).

1. Commencement

This standard shall come into effect on 1 August 2020.

2. Interpretation

The following terms are defined for the purpose of this standard:

a) **"Business Continuity Planning (BCP)"** involves the task of identifying, developing, acquiring, documenting and testing procedures and resources that will ensure continuity of key operations in the event of an accident, disaster, emergency and or threat.

b) **"Cyber risk"** refers to any risk of financial loss, disruption or damage to the reputation of a licensed financial institution that arise due to the failure of its information technology systems.

c) **"External fraud[2]"** is an operational risk event resulting from theft of information, hacking, or forgery by a person external to the licensed financial institution.

d) **"Inherent risk"** means exposure to loss from current or possible future events, or changes in business or economic conditions. The level of risk intrinsic to or present in activity without considering the impact of mitigation through risk management process and controls.

e) "**Licensed financial institution"** (LFI) as defined in the Banking Act 2015.

f) **"Loss Data"** is data collected from an operational risk loss event.

[1] Section 183 of the Banking Act of Anguilla, No 6 of 2015
[2] See Appendix I for more details

g) **"Operational Risk"** is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.[3] The definition includes legal risk[4] but excludes strategic[5] and reputational risk[6].

h) **"Operational Risk Culture"** is the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a LFI's commitment to and style of operational risk management.

i) **"Operational Loss Event"** is a loss resulting from an operational failure.

j) **"Residual Risk"** is the risk remaining after all other *known* risks have been countered, factored in, or mitigated.

k) **"Risk Appetite"** is a high-level determination of how much risk an institution is willing to accept taking into account the risk/return attributes; it is often taken as a forward looking view of risk acceptance.

l) **"Risk Tolerance"** is a more specific determination of the level of variation an institution is willing to accept around business objectives that is often considered to be the amount of risk the institution is prepared to accept. In this document the terms are used synonymously.

m) **"Risk Control Self-Assessment (RCSA)"** is the process of identifying potential risks, designing and implementing controls to manage them.

n) **"Scenario Analysis"** refers to an element of operational risk management that evaluates exposure to high severity events and the plausible losses, as a result of the operational risk.

---

[3] *Principles for the Sound Management of Operational Risk,* Basel Committee on Banking Supervision, June 2011
[4] The potential that unenforceable contracts, lawsuits or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a LFI.
[5] Strategic risk is the risk to earnings or capital arising from adverse business decisions or improper implementation of those decisions.
[6] The potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in customer base, costly litigation, or revenue reduction.

o) **"Secondary Risk"** a risk that arises as a direct outcome of the control implemented to mitigate the risk.

3. Objectives

The prudential standard aim to:

a) Provide guidance on the development of a framework for the sound management of operational risk for licensed financial institutions.
b) Outline measures financial institutions may take to manage risk associated with operational activities.
c) Establish minimum standards with which the Central Bank expects compliance for mitigating risk associated with the bank's operations.

4. Application

This prudential standard applies to all licensed financial institutions. The standard serves as an advisory to shareholders, boards of directors and to the management of institutions licensed under the Banking Act on the minimum standards the ECCB expects licensees to adopt, in respect of their operational risk management framework.

The standards should be read in conjunction with the *Standard for the Outsourcing of Services*, and the *Standard on Corporate Governance*.

The ECCB recognizes that LFIs may implement different risk management practices depending on their size; ownership structure; nature, scope and complexity of operations; and risk profile**.**

5. PRUDENTIAL STANDARD REQUIREMENTS

1. Operational Risk Management

Operational risk is not new or unique to licensed financial institutions, as it is an inherent part of carrying out an operational activity or process and affects all aspects of business activity. There are four main causes of an operational risk event: the person doing the activity makes an error, the process supporting the activity is flawed or not fit for purpose, the system facilitating the activity is broken, or an event external to the institution disrupts the activity.

1.1. Three lines of defence

Sound internal governance forms the foundation of an effective operational risk management framework. Management of operational risk will vary based on the nature, size, complexity of the institutions activities and its risk profile. However, common industry practice for sound operational risk governance often relies on three lines of defence: business line, risk management and an independent review.

1.1.1. Front Line/Business Line

The front line or business line is the first line of defence. The first line has ownership and manages the operational risk it incurs in conducting its activities. The first line of defence is responsible for planning, directing and controlling the day-to-day operations of a significant activity/enterprise-wide process and for identifying and managing the inherent operational risks in products, activities, processes and systems for which it is accountable.

Depending on the size and complexity of the institution, the first line of defence may be responsible for developing the following capabilities:

a. Adherence to the operational risk management framework and related policies;
b. Identification and assessment of the inherent operational risk within their respective business unit and assessing the materiality of risks to the respective business units;
c. Establishment of appropriate mitigating controls and assessing the design and effectiveness of these controls;
d. Oversight of and reports on the business lines' and, operational risk profiles and supporting the operations of the LFI within established operational risk appetite statement;

e. Analysis and reportage of the residual operational risk that is not mitigated by controls, including operational risk events, control deficiencies, human resources, process, and system inadequacies;
f. Promotion of a strong operational risk management culture throughout the first line of defence;
g. Timely and accurate escalation of material issues; and
h. Staff training in their roles in operational risk management if required.

1.1.2. Independent Risk Function

The second line of defence involves oversight activities that objectively identify, measure, monitor and report operational risk on an enterprise basis. The second line challenges or provides an objective assessment of the front/ business lines' inputs and outputs for risk management.

The degree of independence of the second line of defence will differ among institutions. Small institutions may achieve independence through separation of duties and independent review of processes and functions. Larger institutions second line will generally consist of a separate reporting structure independent of the risk generating business lines. Responsibilities associated with the second line include:

a. The design, maintenance and ongoing development of the operational risk framework including but not limited to:
    - strategies to identify, assess, measure, monitor and control/mitigate operational risk; and
    - processes and procedures to provide oversight of operational risk management practices;

b. Operational risk measurement and reporting to the risk committees and the board of directors.
c. Challenging the front/business lines' inputs and outputs regarding the risk management systems.

d. Providing effective objective assessment, which should be evidenced and documented where material risk is identified. For instance, providing examples of the challenges and outcomes so as to be subsequently observable to the first line of defence;
e. Reviewing and monitoring the operational risk profile (this may also include aggregating and reporting);
f. Promoting a strong operational risk management culture throughout the enterprise; and
g. Confirming timely and accurate escalation of material issues;
h. Monitoring the environment for emerging operational risks; and
i. Identifying training gaps and making recommendations to management on training needs.

The function should have a sufficient number of staff skilled in the management of operational risk to effectively address its responsibilities. LFIs should consider implementing quality assurance programmes that ensure an independent challenge is consistently applied to the operational risk management tools, measurement and reporting systems. The involvement of other control groups (such as compliance, legal, business continuity, technology risk management) as subject matter experts to assist with the second line of defence responsibilities should be practiced.

1.1.3. Internal Audit

The internal audit function is charged with the third line of defence. The audit function is separate from the front/business line (first line) and independent risk function (second line). It provides an objective review and testing of the operational risk management controls, processes, systems and the effectiveness of the first and second line of defence functions. Internal audit coverage should be able to verify independently that the framework has been implemented as intended and functions effectively. The internal audit function should:

a. Assess the overall appropriateness and adequacy of the framework and the governance process across the institution;
b. Verify whether the key organisational risk policies and procedures are effective, appropriate and are being complied with;

c. Opine on the overall appropriateness and adequacy of the framework and the associated governance processes in business line;
d. Evaluate whether the framework meets the LFI's needs and regulatory expectations; and
e. Recommend remedial actions in cases of noncompliance and recommend enhancement to policies and procedures where deficiencies exist.

Individuals performing the reviews must be competent and appropriately trained and not involved in the development, implementation and operation of the framework. Where audit activities are outsourced, senior management should consider the effectiveness of the underlying arrangements and the suitability of relying on an outsourced audit function as a third line of defence.

In instances where the internal audit function (particularly smaller institutions) is responsible for developing an operational risk management program, measures should be put in place to ensure that the responsibility for the daily management of operational risk is transferred elsewhere.

2. Governance Framework for Operational Risk Management

LFIs are required to develop, implement and maintain an operational risk management framework. The framework developed would depend on the size, nature and complexity of the activities of the institution. Board and senior management oversight, internal reporting controls and contingency planning are critical elements of an effective framework.

In developing the framework, LFIs should consider its ability to do the following, at a minimum:

a. Define and explain exposures and incidents that result from people, processes, systems, and external events, and generate enterprise-wide understanding of the drivers of operational risk incident;

b. Provide early warning signals of incidents and escalation of potential risk by anticipating risks and identifying problem areas through on-going monitoring of key risk indicators;
c. Reduce vulnerability to external and systemic effects;
d. Clearly define the roles and responsibilities of line personnel in managing operational risk and empower business units to take necessary actions;
e. Strengthen management oversight;
f. Provide objective measurement tools;
g. Integrate qualitative and quantitative data and other information; and
h. Influence business decisions.

Board and senior management are responsible for developing a risk management environment in the institution. While the Board is ultimately responsible for the oversight of the licensed financial institution's management of operational risk, senior management has responsibility for implementing the operational risk management framework approved by the Board.

2.1. Board of Directors Responsibility

The board of directors' responsibilities should include:

a. Promoting a strong operational risk management culture by establishing a corporate culture guided by strong risk management, supported by appropriate standards and incentives for professional and responsible behaviour;
b. Approving and reviewing the risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the institution is willing to assume. Thresholds and limits of the institutions operational activities should be included in the statement;
c. Establishing a code of conduct or an ethics policy, that sets clear expectations for integrity and ethical values of the highest standard and identifying acceptable business practices and prohibited conflicts;
d. Providing clear, guidance to senior management regarding the principles that should underlie the operational risk management framework;

e. Approving the institution's operational risk management framework;
f. Reviewing at least annually, the institution's operational risk management framework to ensure that operational risk is being adequately managed, and that the framework is adjusted to changes in the institution's environment and conforms to industry best practices;
g. Ensuring that the operational risk management framework is subject to effective and comprehensive internal audit by appropriately trained, competent staff who are independent of operational risk management, and ensuring that the scope and frequency of the audit programme is appropriate to the institution's risk exposure;
h. Reviewing and approving audit and supervisory reports on operational risks and following up to ensure deficiencies identified are addressed in a timely manner; and
i. Establishing a committee to provide oversight at the board level for operational risk management. At least one member of the committee should be an independent non-executive member.

2.2. Senior Management Responsibility

Senior management's responsibilities include:

a. Defining the institution's risk appetite and tolerance statement for operational risk;
b. Developing policies, processes and procedures relating to all levels of the LFI's material products, activities, processes and systems that can be implemented and verified within the different business units;
c. Implementing and maintaining a robust system to report, track and when necessary escalate issues to ensure resolution of issues arising from operational risk events;
d. Assessing the appropriateness of management's oversight processes relative to inherent operational risk and ensuring that the necessary resources are available to manage the risk effectively;
e. Ensuring that staff have the necessary experience, technical capabilities and access to resources;
f. Ensuring that staff responsible for monitoring and enforcing compliance with the institution's risk policy have authority independent from the units they oversee;

g. Ensuring that the institution's operational risk management policy has been clearly communicated to staff at all levels and that all levels of staff understand their responsibilities with respect to operational risk management;
h. Facilitating effective communication among staff responsible for risk management, as well as those responsible for the procurement of external services such as insurance purchasing and outsourcing arrangements. Failure to do so could result in significant gaps or overlaps in an LFI's overall risk management programme;
i. Ensuring that the LFI's remuneration policies are consistent with its appetite for risk and do not reward or encourage deviation from policies as this can weaken the risk management processes;
j. Ensuring that policies, processes and procedures related to advanced technologies supporting high transactions volumes are well documented and disseminated to all relevant personnel; and
k. Requiring and reviewing periodic reports from business units and the internal audit function to accurately assess risk exposures against risk tolerances and adherence to internal policies, processes and procedures. Ensuring that reports are distributed to the appropriate levels of management of the institution.
l. Ensuring that the roles and responsibilities of front line management and staff are enhanced with respect to operational risk and that follow up or refresher training is provided.
m. Ensuring that special attention is paid to internal control activities where the LFI engages in new activities or develops new products (particularly where these activities or products are not consistent with the core business strategies), and enter unfamiliar markets. Licensed financial institutions should manage this risk by establishing appropriate business continuity and disaster recovery plans.

3. Risk Management Environment

Operational risk management is the process by which LFIs reduce their operational risk profile to within acceptable levels, as set out by the board and senior management. It is impossible for LFIs to eliminate operational risk; the objective of operational risk management is to minimize

operational risk. Therefore, a certain amount of loss would have to be accepted, based on the LFI's risk appetite. Areas of operation (*Ref. Appendix I*) that should be captured in an operational risk management framework include but are not limited to:

a. Internal fraud;
b. External fraud;
c. Employment practices and workplace safety;
d. Clients, products and business practices;
e. Damage to physical assets;
f. Human losses;
g. Business disruption and system failures; and
h. Execution, delivery and process management.

Management of operational risk includes identification, assessment, monitoring and control/mitigation of risk. A sound operational risk management framework includes effective oversight by the board of directors (the Board), implementation of organisational and procedural controls by senior management and verification by the internal audit function, which provides feedback to the Board.

The framework should be documented in policies and procedures that comprehensively and appropriately define operational risk and operational loss. Institutions must ensure that operational risk is clearly defined and classified, and that loss exposures, thresholds and limits are outlined. The policies should:

a. Identify the governance structures used to manage operational risk, including reporting lines and accountabilities;
b. Describe the risk assessment tools and how they are used;
c. Describe the institution's accepted operational risk profile, permissible thresholds or tolerances for inherent and residual risk, and approved risk mitigation strategies and instruments;
d. Describe the institution's approach to establishing and monitoring thresholds or tolerances for inherent and residual risk exposure;

e. Establish risk reporting and Management Information System (MIS);
f. Provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives;
g. Provide for appropriate independent review and assessment of operational risk; and
h. Require the policies to be revised whenever a material change in the operational risk profile of the institution occurs.
i. Indicate the type of framework implemented for the management of operational risks across subsidiaries of financial conglomerates.
j. Provide for the inclusion of the risks present in non-financial subsidiaries of financial conglomerates.
k. Provide processes and procedures for identifying, assessing, monitoring, reporting and mitigating/controlling operational risk.

3.1. Risk identification and assessment

Risk identification and assessment are fundamental components of an effective operational risk management framework. In the absence of a risk identification and assessment process, licensed financial institutions would be unable to effectively monitor and control key operational risks. Licensees should have a formal process to identify and assess all significant operational risks.

Identification and assessment of operational risk is an ongoing and continuous process and seeks to capture the dynamics of a licensed financial institution and its business. The process should be undertaken at least annually or more frequently, depending on the institution's changing risk profile.

The identification process is a key part of the management of operational risk and should consider all parts of an institution's operation. Once a risk has been identified, institutions can understand its impact and then consider mitigating methods. Licensed financial institutions should identify the inherent risk, residual risk and secondary risk. Institutions should ensure

the real or inherent risk, which needs to be managed, is identified and not the residual or secondary risk.

The risk identification processes should:

a. Identify the significant operational risks to the achievement of the LFI's business objectives;
b. Identify the operational risk inherent in new and existing material products, activities, processes and systems;
c. Focus on the root causes and influencing factors of operational risk, both internal (such as the institution's structure and nature of activities, the quality of the institution's human resources, and employee turnover) and external (such as industry and technological changes), as well as the effects and outcomes: financial, reputational or other;
d. Ensure that the LFI is aware of its major risks at any point in time, and include elements to update its understanding of risk on an on-going basis, using key indicators for various types of operational risk.

In addition to identifying the most significant operational risks, licensed financial institutions should assess their vulnerability to these risks. Risk assessment considers both the likelihood that the risk will occur and the impact of the occurrence.
The assessment process includes understanding losses to the institution if an operational risk event were to occur, whether financial or reputational. The assessment should also consider the effectiveness of the existing controls in mitigating risk identified.

The risk identification and assessment processes should result in the compilation of the institution's operational risk profile. Appropriate risk identification and assessment can be conducted using qualitative or quantitative tools, or a combination of both. Common tools utilised in the identification and assessment of operational risk include:

a. **Audit findings**. Internal audit findings are one of the simplest tools a licensed financial institution can use to identify and assess where it is vulnerable to operational risk.

Audit findings focus on control weaknesses and vulnerabilities, highlighting inherent risks that are present due to internal and external factors.

b. **Loss Event Database**. A loss event database captures and accumulates individual loss events across business units and risk types. Data on a licensed financial institution's historical loss experience could provide information for assessing its exposure to operational risk and developing a policy to mitigate/control the risk. Some firms have also combined internal loss data with external loss data, scenario analyses, and risk assessment factors.

c. **Risk Self-Assessment**. A technique in which management and/or work-teams, identify and assesses risk associated with the underlying process of the LFI's operations and consider the potential impact of the operational risk based on estimates from the consensus of opinions from a group of knowledgeable managers and staff. This process is internally driven and often incorporates checklists, scorecards and/or workshops with the ultimate objective being to foster the ability to identify, assess and mitigate operational risk.

   When risk self-assessment is used, there should be procedures to provide challenge and oversight to ensure opinions are consistently applied across the organization. This is important as there can be significant diversity in judgemental perceptions of risk from person to person.

d. **Risk Mapping**. A technique employed to describe business processes in a clear, visible way. In the context of operational risk, it is designed to provide a reflection of the diverse activities that occur within departments which include; identifying risk drivers, interdependences and controls. It can reveal areas of management weakness and thus help to prioritise subsequent management action.

e. **Risk and Performance Indicators**. Risk and performance indicators are statistics and/or metrics, which can provide insight into an LFI's risk exposure. *Risk indicators* are used to monitor the main drivers associated with the key risks identified by the LFI. *Performance indicators* are measurements, which can provide insight into the operational process, allowing LFIs to identify weaknesses, failures and areas of potential loss.

There are three types of indicators, which are relevant for operational risk management:

i. *Key Performance Indicators* (KPIs) are normally used for monitoring operational efficiency; red flags are triggered if the indicators move outside an established range. Examples: Failed trades, staff turnover, volume, systems downtime.

ii. *Key Control Indicators* (KCIs) demonstrate the effectiveness of controls. Examples: number of audit exceptions and number of outstanding confirmations.

iii. *Key Risk Indicators* (KRIs) are primarily a selection of KPIs and KCIs. This is where performance indicators are tracked alongside control indicators to assess whether the risk is effectively managed. The selection is typically made by risk managers from a pool of business data/indicators considered useful for the purpose of risk tracking. A KRI gives insight on the extent of stress of an activity. KRIs can be used as a time series to monitor and forecast trends. The trend analysis can serve as an early warning system.

f. **Scenario Analysis**. Scenario analysis is an effective tool to consider potential sources of significant operational risk and if additional controls are required. Business line and risk management should work together to develop appropriate scenarios.

g. **Comparative Analysis**. Comparative analysis involves comparing the results of the various assessment tools to give the licensed financial institution a holistic view of its operational risk profile.

A licensed financial institution should utilise a combination of the above tools based on its size and complexity, to ensure it adequately and accurately identifies, and assesses key operational risk drivers, possible control weaknesses and mitigating control measures.

3.2. Risk Monitoring and Reporting

An effective monitoring process is essential for sound operational risk management. Regular monitoring can assist in early detection and correction of deficiencies, thus substantially reducing the potential frequency and/or severity of a loss event. When developing this aspect of the framework, licensed financial institutions should at a minimum:

a. Develop, maintain and utilise a comprehensive management information system to allow management to monitor on an on-going basis operational risk profiles and material exposure to losses;
b. Incorporate regular reporting of exceptional exposures, loss experience and authorised deviations from the operational risk policy to senior management and the Board;
c. Identify appropriate indicators that provide early warning signals of an increased risk of future losses. Such key risk or early warning indicators should be forward-looking and should reflect potential sources of operational risk such as rapid growth, employee turnover and system downtime. Additionally, licensed financial institutions should set appropriate thresholds (or risk tolerances) for these indicators, where possible;
d. Establish a monitoring frequency that reflects the level of risks and momentum of changes in the operating environment;
e. Require business units, group functions and internal audit to report to senior management and the Board on all areas of risk within their purview. These reports should contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making. Any identified problem areas should be fully reflected in the reports, which should motivate timely corrective action on outstanding issues. Reports should be distributed to appropriate levels of management and to areas of the institution on which areas of concern may have an impact.

3.3. Risk control and mitigation

Identifying, assessing and measuring operational risk represent a passive analysis of risk. Licensed financial institutions must therefore take active steps to mitigate and control risks, reducing the frequency of risk events and subsequent impacts. LFIs must ensure strong internal controls in the form of policies, procedures and systems, are in place and appropriate to mitigate risk.

3.3.1. Internal Controls

Internal controls should be designed to provide reasonable assurance that a licensee will have efficient and effective operations, safeguard its assets, produce reliable financial reports and comply with applicable laws and regulations. Control processes and procedures should include a system for ensuring compliance with policies. The following internal control strategies should be implemented, at a minimum, to mitigate operational risks emanating from business activities:

a. Developing and implementing sound and effective operational risk management policies, processes and procedures;
b. Establishing control processes and procedures for ensuring compliance with documented internal policies concerning the risk management system. Principle elements of this could include:
    i. Top-level reviews of the institution's progress towards the stated objectives;
    ii. Verifying compliance with management controls;
    iii. Policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues; and
    iv. A system of documented approvals and authorizations to ensure accountability to an appropriate level of management.
c. Ensuring appropriate segregation of duties. Personnel (or teams) should not be assigned responsibilities which may create a conflict of interest. All areas of potential conflicts of interest should be identified, minimised, and subject to careful independent monitoring and review. Also, efforts should be made to ensure that no one person is in

a position to control sufficient stages of processing a transaction that errors or defalcations could occur without a reasonable chance of detection;

d. Clearly defined and appropriate levels of delegation of authority, risk limits or thresholds;
e. Maintaining safeguards for access to, and use of, the institutions assets and records;
f. Assessing whether returns appear to be out of line with reasonable expectations, for business lines and products (for example, where a supposedly low risk, low margin trading activity generates high returns that would call into question whether such returns have been achieved as a result of internal control breaches);
g. Regular verification and reconciliation of transactions and accounts;
h. Establishing a system of dual control to sensitive areas of the licensed financial institution's operations to ensure that no one individual has complete access to or control of physical assets or sensitive information.
i. Ensuring that there is appropriate processing technology and information technology security to achieve risk mitigation. However, licensed financial institutions should be aware that increased automation could transform high-frequency, low-severity losses into low-frequency, high-severity losses.

In circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management can complement controls by seeking to transfer the risk to another party such as through insurance. The board of directors should determine the maximum loss exposure the bank is willing and has the financial capacity to assume, and should perform an annual review of the bank's risk and insurance management programme.

3.3.2. Information Technology Systems

The effective use and sound implementation of technology can decrease operational risk arising from human errors, through the increase use of automated systems. However, the use of technology and technology related products introduces new risks and exposes institutions to

possible operational and financial losses. Critical system failure, loss of a network, or programming error, can have a catastrophic impact on an institution. Licensees should ensure that these risks are addressed through a sound technology risk and governance framework.

Licensees should have an integrated approach to identify, measure, monitor and manage technology risks. Further, management should ensure the institution has a sound technology infrastructure that meets its current and long-term business requirements. The infrastructure should provide sufficient capacity for normal activity levels and peak hours, ensuring data and system integrity, security and availability and supporting in integrated and comprehensive risk management.

Sound technology risk management is similar to that of operational risk and include:

a. governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the bank's business objectives;
b. policies and procedures that facilitate identification and assessment of risk;
c. establishment of a risk appetite and tolerance statement, as well as performance expectations to assist in controlling and managing risk;
d. implementation of an effective control environment and the use of risk transfer strategies that mitigate risk; and
e. monitoring processes that test for compliance with policy thresholds or limits.

Management should make appropriate capital investment or otherwise provide for a robust technological infrastructure at all times, particularly before high growth strategies are initiated, or new products are introduced. In cases where mergers and acquisitions result in fragmented and disconnected infrastructure, cost-cutting measures or inadequate investment can undermine an institution's ability to aggregate and analyse risk information. Management must take measures to ensure the infrastructure is adequate to manage, oversee and report risk on a consolidated basis.

3.3.3. Outsourcing

Outsourcing in an operational risk context, refers to a licensed financial institution entering into an arrangement or contract with a third party, including an affiliated entity to perform a function or business activity, on a continuing basis that would normally be undertaken by the licensee, now or in the future. Outsourcing can help an institution to manage costs, provide expertise, expand product offerings, and improve services. However, if not adequately managed, outsourcing arrangements can increase the operational risk of a licensed financial institution. The board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in these activities.

Outsourcing may reduce the LFI's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialised business activities. Licensed financial institutions are expected to manage cyber risk exposures that may arise from the outsourcing of business functions. Financial institutions should establish policies for managing the risk associated with outsourcing activities and ensure policies and risk management encompass the following, at a minimum:

a. Sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;
b. Programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider;
c. Establishment of an effective control environment at the bank and the service provider;
d. Development of viable contingency plans; and
e. Oversight by the Board and management to ensure that the third party activity is conducted in a safe and sound manner and in compliance with applicable laws;
f. Requiring the conduct of due diligence tests[7] and monitoring of the activities and performance of third party providers. The extent of the third party's liability and financial capacity to compensate the LFI for errors, negligence, and other operational failures should be explicitly considered as part of the risk assessment;

[7] This should include ensuring that the service provider has the ability, capacity and necessary authorization to perform the outsourced activities reliably and professionally.

g. Ensuring that the service providers have the necessary policies, procedures and practices in place to protect confidential information relating to the LFI and its clients;
h. Robust contracts and/or service level agreements that stipulate and ensure a clear allocation of responsibilities between external service providers and the outsourcing LFI;
i. Access by the LFI, its auditors and relevant regulatory authorities to data related to outsourced activities and the business premises of the service provider

For critical activities, the LFI may need to consider contingency plans, including the availability of alternative external parties and the costs and resources required to switch external parties, potentially on very short notice.

4. Business Continuity Management

Business continuity planning is a key prerequisite for minimising the adverse effects of one of the important areas of operational risk – business disruption and system failures. Licensed financial institutions should develop contingency and business continuity plans to ensure their ability to operate on an on-going basis and limit losses in the event of severe business disruption. The plans should take into account different types of likely or plausible scenarios to which the bank may be vulnerable.

Contingency and business continuity planning should include, inter alia:

a. Identifying critical business processes, including those where there is dependence on external vendors or third parties, for which rapid resumption of service would be most essential. For these processes, licensed financial institutions should identify alternative mechanisms for resuming service in the event of an interruption. Particular attention should be paid to the ability to restore electronic or physical records that are necessary for business resumption;
b. Plausible disruption scenarios should be assessed for financial, operational and reputational impact. The resulting risk assessment should be the foundation for recovery priorities and objectives;

c. Established contingency strategies, recovery and resumption procedures, and communication plans to inform management, employees, regulatory authorities, customer, suppliers and where appropriate civil authorities;
d. Clearly documented and tested processes for shifting resources to secondary/back-up systems and sites;
e. Management succession, emergency powers, predetermined emergency responses and arrangements for the cover and accessibility of key staff members;
f. Capability to revert to existing technology when new software, hardware or telecommunications component is implemented, for example, back out procedures for unsuccessful software upgrades;
g. Specific contingency plans for each outsourcing arrangement based on the degree of materiality of the outsourced activity to the licensed financial institution's business;
h. Periodic review of the disaster recovery and business continuity plans to ensure consistency with the licensed financial institution's current operations and business strategies;
i. Periodic testing of the disaster recovery and business continuity plans to ensure that the licensed financial institution would be able to execute the plans in the unlikely event of a severe business disruption;
j. Insurance coverage for losses occurring from operational risk; and
k. Training and awareness programmes for the effective execution of plans by staff members.

Senior management is responsible for regularly reviewing the plans to make sure they are updated to meet the institutions operational and strategic needs. Results from the business continuity plan and disaster recovery testing should be reported to the board.

5. Role of disclosure

Licensed financial institutions must make sufficient public disclosure to allow market participants to assess their approach to operational risk management. An institution's public disclosure of relevant operational risk management information can lead to transparency and

the development of better industry practice through market discipline. The amount and frequency of disclosure should be commensurate with the size, risk profile and complexity of the licensed financial institution's operations. Licensed financial institutions should implement a board approved disclosure policy, which clearly addresses the institution's approach to operational risk disclosures including the amount and frequency of such disclosures.

The operational risk management framework should be disclosed in a manner that will allow investors and counterparties to determine whether the institution identifies, assesses, monitors and controls/mitigates operational risk effectively.

APPENDIX I

LOSS EVENT TYPE CLASSIFICATION

Event-Type	Definition	Categories	Examples
Internal fraud	Losses due to misappropriation of assets, tax evasion, intentional mismarking of positions, bribery.	Unauthorised Activity	Transactions not reported (intentional) Transaction type unauthorised (w/monetary loss) Mismarking of position (intentional)
		Theft and Fraud	Fraud / credit fraud / worthless deposits Theft / extortion / embezzlement / robbery Misappropriation of assets Malicious destruction of assets Forgery Cheque kiting Smuggling Account take-over / impersonation / etcetera. Tax non-compliance / evasion (wilful) Bribes / kickbacks
External fraud	Losses due to theft of information, hacking damage, third party theft and forgery.	Theft and Fraud	Theft/Robbery Forgery Cheque kiting Cyber attacks Phishing Spoofing ATM Skimming Vishing

Event-Type	Definition	Categories	Examples
		Systems Security	Hacking damage Theft of information (w/monetary loss)
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events	Employee Relations	Compensation, benefit, termination issues Organised labour activity
		Safe Environment	General liability (slip and fall, etcetera.) Employee health & safety rules events Workers compensation
		Diversity & Discrimination	All discrimination types
Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Suitability, Disclosure & Fiduciary	Fiduciary breaches / guideline violations Suitability / disclosure issues (KYC, etcetera.) Retail customer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender liability
		Improper Business or Market Practices	Antitrust Improper trade / market practices Market manipulation Insider trading (on firm's account) Unlicensed activity

Event-Type	Definition	Categories	Examples
			Money laundering
		Product Flaws	Product defects (unauthorised, etcetera.) Model errors
		Selection, Sponsorship & Exposure	Failure to investigate client per guidelines Exceeding client exposure limits
		Advisory Activities	Disputes over performance of advisory activities
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events.	Disasters and other events	Natural disaster losses Human losses from external sources (terrorism, vandalism)
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	Hardware Software Telecommunications Utility outage / disruptions
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution & Maintenance	Miscommunication Data entry, maintenance or loading error Missed deadline or responsibility Model / system misoperation Accounting error / entity attribution error Other task misperformance Delivery failure Collateral management failure

Event-Type	Definition	Categories	Examples
			Reference Data Maintenance
		Monitoring and Reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
		Customer Intake and Documentation	Client permissions / disclaimers missing Legal documents missing / incomplete
		Customer / Client Account Management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
		Trade Counterparties	Non-client counterparty non-performance
		Vendors & Suppliers	Misc. non-client counterparty disputes Outsourcing Vendor disputes